PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-100068
(43)Date of publication of application : 07.04.2000

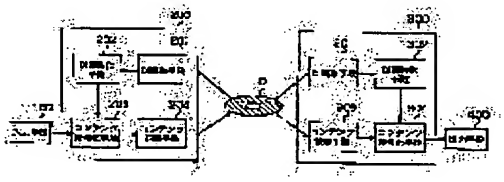
(51)Int.CI. G11B 20/10

(21)Application number : 10-266715
(22)Date of filing : 21.09.1998

(71)Applicant : VICTOR CO OF JAPAN LTD
(72)Inventor : HIRATA ATSUMI
MIYAZAKI TAKESHI
SUZUKI HIDEO

(54) INFORMATION RECORDING METHOD AND DEVICE THEREOF, INFORMATION REPRODUCING DEVICE, INFORMATION PROTECTING METHOD AND INFORMATION RECORDING MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To prevent the unauthorized copy and to permit the reproduction of a properly recorded disk even by any reproducing device by keeping the intrinsic information respectively peculiar for each information recording medium to record on respective information recording media by the unchangeable method and enciphering the information while taking this intrinsic information as a key to record it on the information recording medium.
SOLUTION: When the contents CT are inputted by an input means 100, the intrinsic information DI of the disk D is read by a DI reading means 201 and made to have the functional relation by a DI functionating means 202 to define as F(DI). Then, the contents CT are enciphered by the intrinsic information F(DI) made to have the functional relation to define as E(CT) in a contents enciphering means F(DI) and recording on the disk D by a contents recording means 204. Since the peculiar intrinsic information is previously kept to record and the contents are enciphered by this intrinsic information, the intrinsic information is recorded respectively on the information recording medium, and the contents are reproducible even by the separate reproducing means.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision

of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

未請求中（2003/05/01）

6200002200001000068

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－100068
（P2000－100068A）
(43)公開日　平成12年４月７日(2000.4.7)

(51)Int.Cl.'	識別記号	ＦＩ	ﾃｰﾏｺｰﾄﾞ(参考)
Ｇ１１Ｂ　20/10		Ｇ１１Ｂ　20/10	Ｈ　５Ｄ０４４

審査請求　未請求　請求項の数６　ＯＬ　（全 11 頁）

(21)出願番号　特願平10－266715

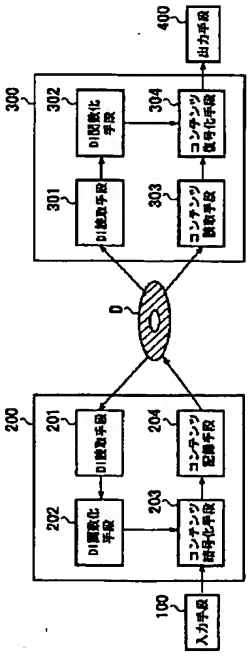
(22)出願日　平成10年９月21日(1998.9.21)

(71)出願人　000004329
日本ビクター株式会社
神奈川県横浜市神奈川区守屋町３丁目12番地
(72)発明者　平田　渥美
神奈川県横浜市神奈川区守屋町３丁目12番地　日本ビクター株式会社内
(72)発明者　宮崎　健
神奈川県横浜市神奈川区守屋町３丁目12番地　日本ビクター株式会社内
(74)代理人　100083806
弁理士　三好　秀和　（外９名）

最終頁に続く

(54)【発明の名称】　情報記録方法、その装置、情報再生装置、情報保護方法及び情報記録媒体

(57)【要約】
【課題】　情報を放送や通信手段を介して伝達し記録型ディスクに記録する際、記録型ディスク媒体から不正にコピーされることを防止することを課題とする。
【解決手段】　ディスクＤに記録された各ディスクそれぞれ特有の固有情報ＤＩによりコンテンツを暗号化してディスクＤに記録し、再生する場合にはディスクＤに記録されている固有情報ＤＩによって暗号化されたコンテンツを復号化することを特徴とする。



1

【特許請求の範囲】

【請求項１】　それぞれ特有の固有情報を改変できない方法でそれぞれの情報記録媒体に記録しておき、この固有情報を鍵として情報を暗号化して前記情報記録媒体に記録することを特徴とする情報記録方法。

【請求項２】　情報記録媒体に情報を暗号化して記録する情報記録装置であって、少なくとも前記情報記録媒体毎にそれぞれ記録された固有情報を読み取る固有情報読み取り手段と、

この固有情報読み取り手段によって読み取られた固有情報によって入力されたコンテンツを暗号化するコンテンツ暗号化手段と、

このコンテンツ暗号化手段によって暗号化されたコンテンツを前記情報記録媒体に記録するコンテンツ記録手段とから構成されることを特徴とする情報記録装置。

【請求項３】　情報記録媒体に記録された情報を復号化して再生する情報再生装置であって、少なくとも前記情報記録媒体毎にそれぞれ記録された固有情報を読み取る固有情報読み取り手段と、

前記情報記録媒体に記録された暗号化されたコンテンツを読み取るコンテンツ読み取り手段と、

このコンテンツ読み取り手段によって読み取られた前記暗号化されたコンテンツを前記固有情報によって復号化して出力するコンテンツ復号化手段とから構成されることを特徴とする情報再生装置。

【請求項４】　それぞれ特有の固有情報を改変できない方法でそれぞれの情報記録媒体に記録しておき、この固有情報を鍵として情報を暗号化して前記情報記録媒体に記録し、この暗号化して記録された情報を前記固有情報によって復号して再生することを特徴とする情報保護方法。

【請求項５】　前記固有情報と認証用の情報とから認証子を生成し、前記情報記録媒体に記録されている認証子と同一であるか否かを判断することをさらに含むことを特徴とする請求項４に記載の情報保護方法。

【請求項６】　各情報記録媒体毎にそれぞれ特有の固有情報が改変できない方法で、あるいは改変できないエリアに記録されていることを特徴とする情報記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、記録型ディスクに記録された情報を保護するための情報保護装置及びその方法に関し、特に個々のディスクに特有の固有情報をディスクに記録することによって、不正コピーを防止する情報を保護する方法に関する。

【０００２】

【従来の技術】ＣＤ－Ｒ，ＰＤ，ＤＶＤ－ＲＡＭ，ＤＶＤ－ＲＷなどの記録型ディスク媒体（以下ディスクという）及び装置において、ネットワークあるいは放送を介して伝送され、正当に権利を得て１回記録することを許

2

された場合、映画などの動画像、静止画像、音楽などのコンテンツは簡単に記録することができなければならない。また、記録後のディスクは、正規の装置であればどの装置を利用しても再生できるようにしたいという要求がある。

【０００３】一方、そのような記録型ディスク媒体及び装置において、不正にコピーされることを防止して著作権を守る必要があるが、正当な権利で容易に記録・再生できることとコピーを防止することは背反しており両立させることが困難であった。

【０００４】そこで、このような矛盾を解決すべく従来の情報保護装置では、ユーザーＩＤを利用することによって不正なコピーを防止していた。

【０００５】図６に示すように、従来の情報保護装置は、動画像、静止画像、音楽などのコンテンツを入力する入力手段１０と、一般的な情報記録媒体Ｄにコンテンツなどの情報を暗号化して記録する情報記録手段２０と、情報記録媒体Ｄに記録された情報を復号化して再生する情報再生手段３０と、復号化されたコンテンツなどの情報を出力する出力手段４０とを含んでいる。

【０００６】ここで、情報記録手段２０は、情報再生手段３０からネットワーク５０を介して送られてくるユーザーＩＤ（ＵＩ）を読み取るＵＩ読み取り手段２１と、入力手段１０により入力されるコンテンツを暗号化するための鍵ＫＥＹを保持する鍵保持手段２２と、この鍵保持手段２２に保持された鍵ＫＥＹをＵＩ読み取り手段２１によって読み取られたユーザーＩＤによって暗号化する鍵暗号化手段２３と、この鍵暗号化手段２３によって暗号化された鍵Ｅ（ＫＥＹ）をネットワーク５０を介して情報記録媒体Ｄに記録する鍵記録手段２４と、鍵保持手段２２に保持された鍵ＫＥＹによって入力手段１０から入力されたコンテンツＣＴを暗号化するコンテンツ暗号化手段２５と、このコンテンツ暗号化手段２５によって暗号化されたコンテンツＥ（ＣＴ）をネットワーク５０を介して情報記録媒体Ｄに記録するコンテンツ記録手段２６とから構成されている。

【０００７】また、情報再生手段３０は、ユーザーＩＤ（ＵＩ）を保持し、ネットワークを介して伝送するＵＩ保持手段３１と、情報記録媒体Ｄに記録された暗号化された鍵Ｅ（ＫＥＹ）を読み取る鍵読み取り手段３２と、この鍵読み取り手段３２によって読み取られた暗号化された鍵Ｅ（ＫＥＹ）をユーザーＩＤによって復号化する鍵復号化手段３３と、復号化された鍵を保持する鍵保持手段３４と、情報記録媒体Ｄに記録された暗号化されたコンテンツＥ（ＣＴ）を読み取るコンテンツ読み取り手段３５と、このコンテンツ読み取り手段３５によって読み取られた暗号化されたコンテンツＥ（ＣＴ）を鍵保持手段３４に保持された鍵ＫＥＹによって復号化して出力手段４０へ出力するコンテンツ復号化手段３６とから構成されている。

3

【０００８】次に従来の情報保護装置の動作を説明する。

【０００９】コンテンツＣＴが入力手段１０より入力されると、コンテンツ暗号化手段２５において、コンテンツＣＴは鍵保持手段２２に保持されている鍵ＫＥＹによって暗号化されてＥ(ＣＴ)となり、コンテンツ記録手段２６によってネットワーク５０を介してディスクＤに記録される。

【００１０】一方、ユーザーがそれぞれ固有に持つユーザーＩＤ（ＵＩ）はネットワーク５０を介してＵＩ保持手段３１からＵＩ読み取り手段２１に送られ、鍵暗号化手段２３において、鍵保持手段２２に保持された鍵ＫＥＹを暗号化してＥ(ＫＥＹ)とする。この暗号化された鍵Ｅ(ＫＥＹ)は鍵記録手段２４によってネットワーク５０を介してディスクＤに記録される。

【００１１】そして、ユーザーは情報再生手段３０において、ディスクＤを再生する。まずディスクＤから鍵読み取り手段３２によって暗号化された鍵Ｅ(ＫＥＹ)が読み取られ、次に鍵復号化手段３３において暗号化された鍵Ｅ(ＫＥＹ)をユーザーＩＤによって復号化して鍵ＫＥＹを得て鍵保持手段３４に保持する。また、暗号化されたコンテンツＥ(ＣＴ)はコンテンツ読み取り手段３５によって読み取られ、コンテンツ復号化手段３６において、鍵保持手段３４に保持されている鍵ＫＥＹにより復号化されてコンテンツＣＴとなり、出力手段４０に送られ出力されることになる。

【００１２】

【発明が解決しようとする課題】しかしながら、このような従来の情報保護装置では、情報再生手段３０に特有のユーザーＩＤによって鍵ＫＥＹを暗号化してディスクＤに記録していたため、ディスクＤは他の情報再生手段ではユーザーＩＤが異なるため再生することができず、例えばユーザーが情報再生手段であるプレーヤーを買い換えた場合や増設した場合にディスクＤを再生することができないという問題点があった。

【００１３】そこで、他のプレーヤーでも再生ができるようにユーザーＩＤをディスクＤに記録することが考えられる。

【００１４】しかしながら、ユーザーＩＤをディスクに記録すると、確かに図７の点線で示すようにＵＩ保持手段３１がディスクＤからユーザーＩＤを読み取ることによって他のプレーヤでもディスクＤを再生できるようにはなるものの、ディスクＤを丸ごとコピーすることによって不正なコピーディスクＤ’が容易に作れることになり情報の保護ができなくなるという別の問題点が生じることになっていた。

【００１５】本発明は上記事情に鑑みてなされたものであり、その目的は、ネットワークあるいは放送を介して伝送されたコンテンツを正当に認められた権利によって記録したディスクから、別のディスクや記録媒体に不正

4

コピーすることを防止するとともに、正当に記録したディスクはどの再生装置でも再生することのできる情報保護装置、その方法及び情報保護するための情報記録媒体を提供することにある。

【００１６】

【課題を解決するための手段】上記目的を達成するために、第１の発明である情報記録方法は、各情報記録媒体にそれぞれ特有の固有情報を改変できない方法でそれぞれの情報記録媒体に記録しておき、この固有情報を鍵として情報を暗号化して前記情報記録媒体に記録することを特徴とする。

【００１７】この第１の発明によれば、不正コピーを防止できるとともに、正当に記録したディスクはどの再生装置においても再生することができる。

【００１８】第２の発明である情報記録装置は、情報記録媒体に情報を暗号化して記録する情報記録装置であって、前記情報記録媒体毎にそれぞれ記録された固有情報を読み取る固有情報読み取り手段と、この固有情報読み取り手段によって読み取られた固有情報によって入力されたコンテンツを暗号化するコンテンツ暗号化手段と、このコンテンツ暗号化手段によって暗号化されたコンテンツを前記情報記録媒体に記録するコンテンツ記録手段とから構成されることを特徴とする。

【００１９】この第２の発明によれば、不正コピーを防止できるとともに、正当に記録したディスクはどの再生装置においても再生することができる。

【００２０】第３の発明である情報再生装置は、情報記録媒体に記録された情報を復号化して再生する情報再生装置であって、前記情報記録媒体毎にそれぞれ記録された固有情報を読み取る固有情報読み取り手段と、前記情報記録媒体に記録された暗号化されたコンテンツを読み取るコンテンツ読み取り手段と、このコンテンツ読み取り手段によって読み取られた前記暗号化されたコンテンツを前記固有情報によって復号化して出力するコンテンツ復号化手段とから構成されることを特徴とする。

【００２１】この第３の発明によれば、不正コピーを防止できるとともに、正当に記録したディスクはどの再生装置においても再生することができる。

【００２２】第４の発明である情報保護方法は、各情報記録媒体にそれぞれ特有の固有情報を改変できない方法でそれぞれの情報記録媒体に記録しておき、この固有情報を鍵として情報を暗号化して前記情報記録媒体に記録し、この暗号化して記録された情報を前記固有情報によって復号して再生することを特徴とする。

【００２３】この第４の発明によれば、不正コピーを防止できるとともに、正当に記録したディスクはどの再生装置においても再生することができる。

【００２４】第５の発明である情報保護方法は、前記固有情報と認証用の情報とから認証子を生成し、前記情報記録媒体に記録されている認証子と同一であるか否かを

5

判断することをさらに含むことを特徴とする。

【００２５】この第５の発明によれば、認証子が同一であるか否かを判断することにより固有情報が変更された場合でも検出することができるので、不正なコピーをさらに防止することができる。

【００２６】第６の発明である情報記録媒体は、各情報記録媒体毎にそれぞれ特有の固有情報が改変できない方法で、あるいは改変できないエリアに記録されていることを特徴とする情報記録媒体。

【００２７】この第６の発明によれば、不正コピーを防止できるとともに、正当に記録したディスクはどの再生装置においても再生することができる。

【００２８】

【発明の実施の形態】以下、本発明に係る情報保護装置の第１の実施形態を図面に基づいて説明する。本実施形態の情報保護装置は、各情報記録媒体にそれぞれ特有の固有情報をあらかじめ記録しておき、この固有情報によってコンテンツを暗号化するものである。

【００２９】図１は本実施形態の情報保護装置の構成を示すブロック図である。図１に示すように、本実施形態の情報保護装置は、動画像、静止画像、音楽などのコンテンツを入力する入力手段１００と、一般的な情報記録媒体Ｄにコンテンツなどの情報を暗号化して記録する情報記録手段２００と、情報記録媒体に記録された情報を復号化して再生する情報再生手段３００と、復号化されたコンテンツなどの情報を出力する出力手段４００とを含んでいる。

【００３０】ここで、情報記録手段２００は、情報記録媒体Ｄ毎にそれぞれ記録された固有情報ＤＩを読み取るＤＩ読み取り手段２０１と、このＤＩ読み取り手段２０１によって読み取られた固有情報ＤＩを関数化するＤＩ関数化手段２０２と、このＤＩ関数化手段２０２によって関数化された固有情報Ｆ(ＤＩ)によって入力手段１００から入力されたコンテンツＣＴを暗号化するコンテンツ暗号化手段２０３と、このコンテンツ暗号化手段２０３によって暗号化されたコンテンツＥ(ＣＴ)を情報記録媒体Ｄに記録するコンテンツ記録手段２０４とから構成されている。

【００３１】また情報再生手段３００は、情報記録媒体Ｄ毎にそれぞれ記録された固有情報ＤＩを読み取るＤＩ読み取り手段３０１と、このＤＩ読み取り手段３０１によって読み取られた固有情報ＤＩを関数化するＤＩ関数化手段３０２と、情報記録媒体Ｄに記録された暗号化されたコンテンツＥ(ＣＴ)を読み取るコンテンツ読み取り手段３０３と、このコンテンツ読み取り手段３０３によって読み取られた暗号化されたコンテンツＥ(ＣＴ)を関数化された固有情報Ｆ(ＤＩ)によって復号化して出力手段４００へ出力するコンテンツ復号化手段３０４とから構成されている。

【００３２】次に、本実施形態の情報保護装置の動作について説明する。

6

【００３３】まず、コンテンツＣＴが入力手段１００より入力されると、ディスクＤの固有情報ＤＩをＤＩ読み取り手段２０１が読み取り、この固有情報ＤＩをＤＩ関数化手段２０２で関数化してＦ(ＤＩ)とする。そして、コンテンツ暗号化手段２０３において、入力されたコンテンツＣＴを関数化された固有情報Ｆ(ＤＩ)で暗号化してＥ(ＣＴ)とし、コンテンツ記録手段２０４によってディスクＤに記録する。

【００３４】そして、ユーザーは情報再生手段３００においてディスクＤを再生する場合には、まずディスクＤからＤＩ読み取り手段３０１によってディスクＤの固有情報ＤＩを読み取り、この固有情報ＤＩをＤＩ関数化手段３０２で関数化してＦ(ＤＩ)とする。そして、次に暗号化されたコンテンツＥ(ＣＴ)をコンテンツ読み取り手段３０３によってディスクＤから読み取り、コンテンツ復号化手段３０４において関数化された固有情報Ｆ(ＤＩ)によって復号化してコンテンツＣＴとし、出力手段４００に送り、出力することになる。

【００３５】尚、本実施形態ではＤＩ関数化手段２０２によって固有情報ＤＩを関数化し、この関数化された固有情報Ｆ(ＤＩ)によってコンテンツＣＴを暗号化しているが、固有情報ＤＩを関数化せずに直接固有情報ＤＩによってコンテンツＣＴを暗号化することもできる。この場合には情報再生手段３００においても固有情報ＤＩを関数化することなく、固有情報ＤＩによってコンテンツＣＴを復号化する。

【００３６】このように、本実施形態の情報保護装置では、各情報記録媒体にそれぞれ特有の固有情報をあらかじめ記録しておき、この固有情報によってコンテンツを暗号化するので、ユーザーが情報再生手段を買い換えたり増設した場合でも、固有情報は情報記録媒体にそれぞれ記録されているので、別の情報再生手段でもコンテンツを再生することができる。

【００３７】また、不正なコピーディスクを作成しようとして、ディスクを丸ごとコピーしたとしても、コピーされたディスクを再生しようとすると、固有情報は各ディスク毎に特有のものであるから、暗号化されたときの固有情報と復号化するときの固有情報が異なってしまうためにコンテンツを復号することができない。従って、不正なコピーディスクの作成を防止することもできる。

【００３８】ここで、このような本実施形態の情報保護装置の効果を発揮させるためには、情報記録媒体に記録されている固有情報ＤＩが容易に改竄できない方法で記録されていなければならない。そこで、この固有情報ＤＩについて説明する。

【００３９】同心円状あるいはスパイラル状に情報を記録する任意の追記型あるいは書換型の一般的な情報記録媒体（以下、ディスク媒体と証する）は、図２に示すように、一般利用者は記録することができない領域、すな

7

わちＢＣＡ（バースト・カッティング・エリア）３やリードインエリア２などとユーザーが記録できる領域、データエリア１などで構成されることが多い。このようなディスク媒体において、固有情報ＤＩ（番号・記号・文字・データなど任意の形態でよい）を特定のエリアに記録するか、あるいは例えばディスク媒体生産時に記録しておく方式を用いることによって、ディスク媒体それぞれを識別することが可能となる。

【００４０】ここで、固有情報ＤＩとは、各ディスク媒体をそれぞれ識別可能な唯一、あるいは他のディスク媒体の固有情報ＤＩとは容易に一致しない情報のことである。また、特定のエリアとは、例えば図２のＢＣＡ（バースト・カッティング・エリア）３，リードインエリア２，データエリア１などに記録することができるが、これらの場所に限らず任意の場所に記録することができるものである。

【００４１】このような固有情報ＤＩは、ユーザーが記録できない、あるいは記録されているものを改竄できない方法で記録することが必要であり、例えばディスク上に機械的な凹凸であらかじめ記録しておいたり、強いレーザー光のオンオフなどでディスクの微小領域の組成や破壊による反射率の変化で記録したり、あらかじめ機械的に記録されている信号の一部を破壊するなどの方法で記録することができる。

【００４２】次に、本発明に係る情報保護装置の第２の実施形態を図面に基づいて説明する。本実施形態の情報保護装置は、固有情報とは別の鍵を使ってコンテンツを暗号化するものである。

【００４３】図３は本実施形態の情報保護装置の構成を示すブロック図である。図３に示すように、本実施形態の情報保護装置は、動画像、静止画像、音楽などのコンテンツを入力する入力手段１００と、一般的な情報記録媒体Ｄにコンテンツなどの情報を暗号化して記録する情報記録手段２００と、情報記録媒体に記録された情報を復号化して再生する情報再生手段３００と、復号化されたコンテンツなどの情報を出力する出力手段４００とを含んでいる。

【００４４】ここで、情報記録手段２００は、情報記録媒体Ｄ毎にそれぞれ記録された固有情報ＤＩを読み取るＤＩ読み取り手段２０１と、このＤＩ読み取り手段２０１によって読み取られた固有情報ＤＩを関数化するＤＩ関数化手段２０２と、入力されるコンテンツＣＴを暗号化するための鍵ＫＥＹを保持する鍵保持手段２０５と、この鍵保持手段２０５により保持された鍵ＫＥＹを関数化された固有情報Ｆ（ＤＩ）によって暗号化する鍵暗号化手段２０６と、この鍵暗号化手段２０６によって暗号化された鍵Ｅ（ＫＥＹ）を情報記録媒体Ｄに記録する鍵記録手段２０７と、鍵保持手段２０５により保持された鍵ＫＥＹによって入力手段１００から入力されたコンテンツＣＴを暗号化するコンテンツ暗号化手段２０３と、この

8

コンテンツ暗号化手段２０３によって暗号化されたコンテンツＥ（ＣＴ）を情報記録媒体Ｄに記録するコンテンツ記録手段２０４とから構成されている。

【００４５】また情報再生手段３００は、情報記録媒体Ｄ毎にそれぞれ記録された固有情報ＤＩを読み取るＤＩ読み取り手段３０１と、このＤＩ読み取り手段３０１によって読み取られた固有情報ＤＩを関数化するＤＩ関数化手段３０２と、情報記録媒体Ｄに記録された暗号化された鍵Ｅ（ＫＥＹ）を読み取る鍵読み取り手段３０５と、暗号化された鍵Ｅ（ＫＥＹ）を関数化された固有情報Ｆ（ＤＩ）によって復号化する鍵復号化手段３０６と、この鍵復号化手段３０６によって復号化された鍵ＫＥＹを保持する鍵保持手段３０７と、コンテンツ記録手段２０４によって情報記録媒体Ｄに記録された暗号化されたコンテンツＥ（ＣＴ）を読み取るコンテンツ読み取り手段３０３と、暗号化されたコンテンツＥ（ＣＴ）を鍵保持手段３０７に保持された鍵ＫＥＹによって復号化して出力手段４００へ出力するコンテンツ復号化手段３０４とから構成されている。

【００４６】次に、本実施形態の情報保護装置の動作について説明する。

【００４７】まず、コンテンツＣＴが入力手段１００より入力されると、コンテンツ暗号化手段２０３において、入力されたコンテンツＣＴを鍵保持手段２０５に保持された鍵ＫＥＹによって暗号化してＥ（ＣＴ）とし、コンテンツ記録手段２０４によってディスクＤに記録する。一方、ＤＩ読み取り手段２０１ではディスクＤの固有情報ＤＩを読み取り、この固有情報ＤＩをＤＩ関数化手段２０２で関数化してＦ（ＤＩ）とする。そして、鍵暗号化手段２０６において、鍵保持手段２０５で保持された鍵ＫＥＹを暗号化してＥ（ＫＥＹ）とし、鍵記録手段２０７によってディスクＤに記録する。

【００４８】そして、ユーザーは情報再生手段３００においてディスクＤを再生する場合には、まずディスクＤからＤＩ読み取り手段３０１によってディスクＤの固有情報ＤＩを読み取り、この固有情報ＤＩをＤＩ関数化手段３０２で関数化してＦ（ＤＩ）とする。そして、鍵読み取り手段３０５によって読み取られた暗号化された鍵Ｅ（ＫＥＹ）を、鍵復号化手段３０６において関数化された固有情報Ｆ（ＤＩ）で復号化して鍵ＫＥＹとし、鍵保持手段３０７に保持する。

【００４９】一方、暗号化されたコンテンツＥ（ＣＴ）はコンテンツ読み取り手段３０３によってディスクＤから読み取られ、コンテンツ復号化手段３０４において鍵保持手段３０７に保持された鍵ＫＥＹによって復号化してコンテンツＣＴとし、出力手段４００に送られ出力されることになる。

【００５０】尚、本実施形態ではＤＩ関数化手段２０２によって固有情報ＤＩを関数化し、この関数化された固有情報Ｆ（ＤＩ）によってコンテンツＣＴを暗号化してい

9

るが、固有情報ＤＩを関数化せずに直接固有情報ＤＩによってコンテンツＣＴを暗号化することもできる。この場合には情報再生手段３００においても固有情報ＤＩを関数化することなく、固有情報ＤＩによってコンテンツＣＴを復号化する。

【００５１】このように、第２の実施形態の情報保護装置では、固有情報によってコンテンツを暗号化するのではなく、別に保持されている鍵でコンテンツを暗号化し、この鍵を固有情報で暗号化するので、第１の実施形態の情報保護装置と同様にユーザーが情報再生手段を買い換えたり増設した場合でもコンテンツを再生することができ、不正なコピーディスクの作成も防止できるとともに、さらに情報の保護が確実となる。

【００５２】また、図１と図３に示す第１及び第２の実施形態の情報保護装置において、ネットワーク（放送型、ポイント・ツー・ポイント型、バスラインなど任意の形態を含む）を介してコンテンツを伝送する場合について、図４、図５にそれぞれ示す。基本的な構成は図１、図３と同じでディスクＤに記録する際にネットワーク５００が介在する。

【００５３】次に、情報記録媒体に固有情報ＤＩだけでなく認証子を記録する場合について説明する。

【００５４】追記型ディスク媒体では、ある物理アドレスに一度記録したデータは破壊することはできても、その同じ物理アドレスに異なるデータを記録することはできないので改竄される心配はないが、書き換え可能のディスクの場合にはある物理アドレスに記録した固有情報を故意あるいは不意に変更されてしまうことがあるので固有情報の改竄が問題となる。

10

【００５５】この問題点を解決するために、固有情報と認証用の別の情報とに適当な関数を作用させて、その関数値、すなわちその関数の出力値を認証子として特定のエリアに記録する。固有情報が変更されている場合には認証子が異なってしまうため、固有情報が変更されたことを検出することができる。

【００５６】この方法に用いることができる関数は、固有情報が変化すると出力値が変化し、さらに別の認証用の情報が変化しても出力値が変化するような関数であれば任意の関数を用いることができる。このような機能を持つ関数としては、ＳＨＡ，ＭＤ５などの任意のハッシュ関数や、ブロック暗号ＤＥＳ、公開鍵暗号ＲＳＡなどの任意の暗号関数をＣＢＣ（サイファーブロックチェイニング）モード，ＯＦＢ（アウトプットフィードバック）モード，ＣＦＢ（サイファーフィードバック）モードなどがある。また、ここで用いる関数は任意の長さの入力を扱うことができる関数を用いることもできるので、認証用の別の情報にはディスク内の任意のエリアで任意の長さの情報を使うことができる。また、この関数の出力（関数値）である認証子は、図２のＢＣＡ３（バースト・カッティング・エリア）、リードインエリア２、データエリア１などに記録することができるが、これらの場所に限らず任意の場所に記録してもよい。

【００５７】ここで、認証子の具体例を説明すると、例えば当該固有の情報

“fedcba98 76543210”

が、データエリア最終セクタ先頭に記録されていて、別の認証用の情報

“12345678 9abcdef0　12345678 9abcdef0　12345678 9abcdef0
12345678 9abcdef0　12345678 9abcdef0　12345678 9abcdef0
12345678 9abcdef0　12345678 9abcdef0”

がリードインエリアの一部または全部であるとして、これら２つの情報を統合し、

“12345678 9abcdef0　12345678 9abcdef0　12345678 9abcdef0
12345678 9abcdef0　12345678 9abcdef0　12345678 9abcdef0
12345678 9abcdef0　12345678 9abcdef0
fedcba98 76543210”

これを関数の入力とする。

【００５８】ここで、入力する関数がハッシュ関数　ＳＨＡ－１［１］であると仮定すると、その出力値（認証子）は、

“f18ea0b5　a80901bf　d348fa03　4c173b88　eb4e2191”

となる。この認証子をデータエリア内に記録する。例えば、当該固有情報がデータエリア最終セクタ先頭に記録されていると仮定し、それに続いて同じセクタ内に、この認証子を記録しておくこともできる。

【００５９】次に、このように記録された認証子を利用して、固有情報が変更されていないか検査する。まず、ある特定エリアにある当該固有情報と、ある特定エリアにある認証用の別の情報とをある関数に入力する。そして、その関数の出力値がある特定エリアにある認証子と等しくなれば、記録されている固有情報は正しいと認証し、等しくなければ記録されている固有情報は誤っていると認証することができる。

【００６０】また、固有情報の記録されたディスク媒体では、従来のディスク記録・再生装置においても、データエリアにあるデータを読みとるためには、ソフトウェアやファームウェアの変更のみで、ハードウェアの変更無しに読みとることができる。具体的には、例えばデータエリアの最終セクタ、あるいはこれ以上記録しないであろうという適当なセクタに固有情報を記録し、リードアウトフラグをそのセクタの前あるいはそのセクタ内の

11

先頭に記録することで実現することができる。このように、データエリアの最終セクタに固有情報を記録しておけば、再生すべきデータの後に記録することになるので、このようなディスク媒体を従来のディスク記録・再生装置で再生する場合には、何ら通常のディスクと変わらずに再生することができる。これ以上記録しないであろうという適当なセクタに固有情報を記録した場合も同様である。ただ、固有情報を最終セクタに記録した場合が最も効率が良くなり、セクタのサイズが例えば２Ｋバイトの時は、データエリアが２Ｋバイト小さくなるだけである。

【００６１】別の方法としては、リードインエリア内にリードイン情報とは別に固有情報を記録しておくこともでき、バーストカッティングエリアに記録することもできる。　ここで、バーストカッティングエリアとは、ディスク最内周に位置し、非同期で読み取ることを仮定しているエリアのことで、機能が等しければバーストカッティングエリアという名称には捕らわれないものである。

【００６２】また、バーストカッティングエリアを読みとる仕様になっていない従来のディスク記録・再生装置においては、もともとバーストカッティングエリアを無視して再生するので、従来のディスク記録・再生装置で再生する場合には何ら通常のディスクと変わらずに再生することができる。

【００６３】

【発明の効果】以上説明したように、本発明の情報保護装置、その方法及び情報保護するための情報記録媒体によれば、各情報記録媒体にそれぞれ特有の固有情報をあらかじめ記録しておき、この固有情報によってコンテンツを暗号化するので、ユーザーが情報再生手段を買い換えたり増設した場合でも、固有情報は情報記録媒体に記録されているので、別の情報再生手段でもコンテンツを再生することができる。

【００６４】また、不正なコピーディスクを作成しようとして、ディスクを丸ごとコピーしたとしても、コピーされたディスクを再生しようとすると、固有情報は各ディスク毎に特有のものであるから、暗号化されたときの固有情報と復号化するときの固有情報が異なってしまうためにコンテンツを復号することができない。従って、不正なコピーディスクの作成を防止することもできる。

【００６５】さらに、固有情報だけでなく別の鍵をも利用してコンテンツを暗号化することにより、不正コピーを防止でき、正当に記録したディスクはどの再生装置においても再生することができるとともに、さらに情報の保護が確実となる。

12

【００６６】また、認証子が同一であるか否かを判断することにより固有情報が変更された場合でも検出することができるので、不正なコピーをさらに防止することもできる。

【図面の簡単な説明】

【図１】本発明による情報保護装置の第１の実施形態の構成を示すブロック図である。

【図２】情報記録媒体であるディスクの構成を示す図である。

【図３】本発明による情報保護装置の第２の実施形態の構成を示すブロック図である。

【図４】図１に示す情報保護装置の第１の実施形態において、ネットワークを介する場合における構成を示すブロック図である。

【図５】図３に示す情報保護装置の第２の実施形態において、ネットワークを介する場合における構成を示すブロック図である。

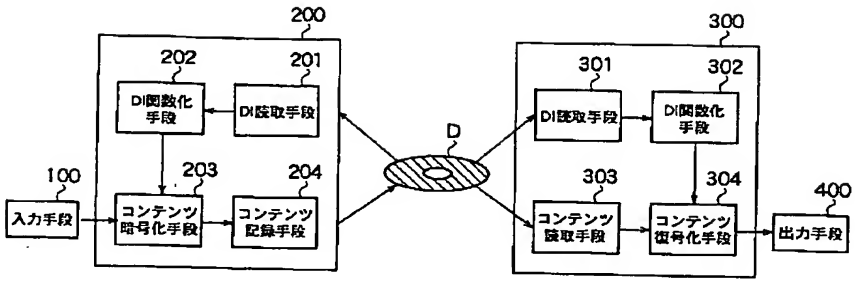
【図６】従来の情報保護装置の構成を示すブロック図である。

【図７】図６に示す従来の情報保護装置において、ユーザーＩＤをディスクに記録した場合を説明するためのブロック図である。

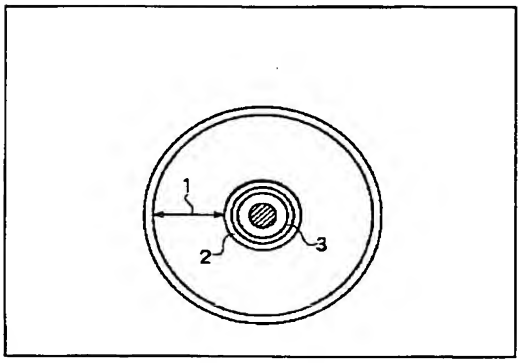
【符号の説明】

１　データエリア
２　リードインエリア
３　バースト・カッティング・エリア
１０、１００　入力手段
２０、２００　情報記録手段
２１　ＵＩ読み取り手段
２２、２０５　鍵保持手段
２３、２０６　鍵暗号化手段
２４、２０７　鍵記録手段
２５、２０３　コンテンツ暗号化手段
２６、２０４　コンテンツ記録手段
３１　ＵＩ保持手段
３２、３０５　鍵読み取り手段
３３、３０６　鍵復号化手段
３４、３０７　鍵保持手段
３５、３０３　コンテンツ読み取り手段
３６、３０４　コンテンツ復号化手段
３０、３００　情報再生手段
４０、４００　出力手段
５０、５００　ネットワーク
２０１、３０１　ＤＩ読み取り手段
２０２、３０２　ＤＩ関数化手段
Ｄ　情報記録媒体

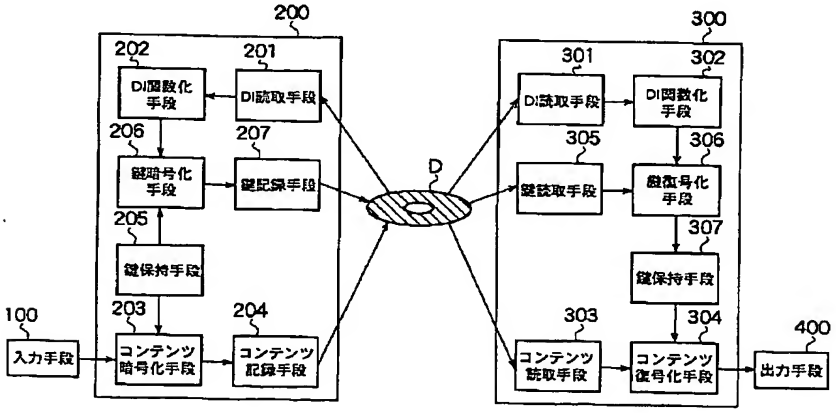
【図１】


200
202
201
DI関数化手段
DI読取手段
100
入力手段
203
204
コンテンツ暗号化手段
コンテンツ記録手段
D
300
301
302
DI読取手段
DI関数化手段
303
304
コンテンツ読取手段
コンテンツ復号化手段
400
出力手段

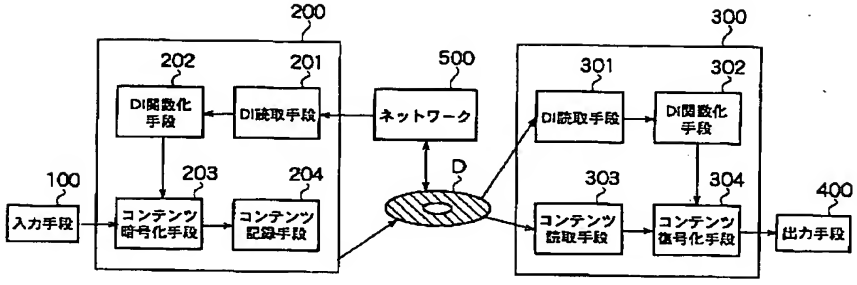
【図２】


1
2
3

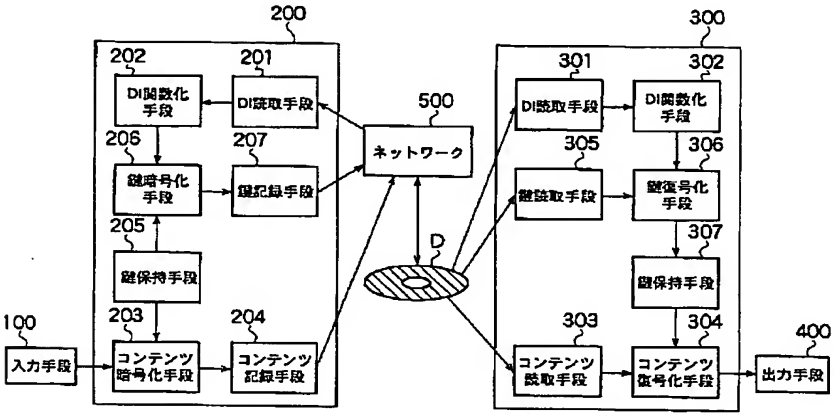
【図３】


200
202
201
DI関数化手段
DI読取手段
206
207
鍵暗号化手段
鍵記録手段
205
鍵保持手段
100
入力手段
203
204
コンテンツ暗号化手段
コンテンツ記録手段
D
300
301
302
DI読取手段
DI関数化手段
305
306
鍵読取手段
鍵復号化手段
307
鍵保持手段
303
304
コンテンツ読取手段
コンテンツ復号化手段
400
出力手段

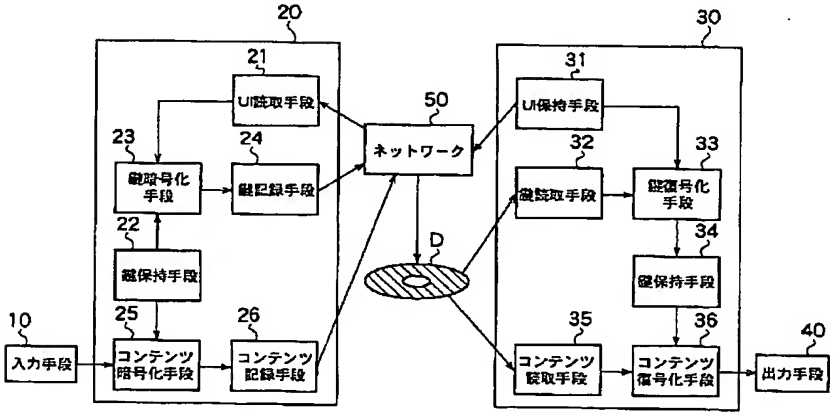
【図４】


200
202
201
500
300
301
302
DI関数化手段
DI読取手段
ネットワーク
DI読取手段
DI関数化手段
100
203
204
D
303
304
400
入力手段
コンテンツ暗号化手段
コンテンツ記録手段
コンテンツ読取手段
コンテンツ復号化手段
出力手段

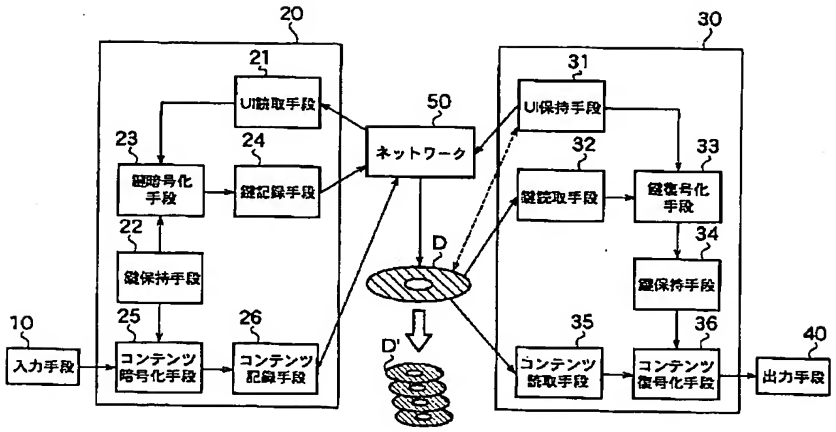
【図５】


200
300
202
201
301
302
DI関数化手段
DI読取手段
500
DI読取手段
DI関数化手段
206
207
305
306
鍵暗号化手段
鍵記録手段
ネットワーク
鍵読取手段
鍵復号化手段
205
D
307
鍵保持手段
鍵保持手段
100
203
204
303
304
400
入力手段
コンテンツ暗号化手段
コンテンツ記録手段
コンテンツ読取手段
コンテンツ復号化手段
出力手段

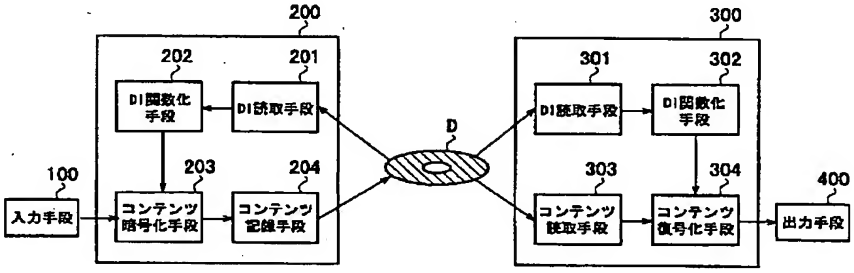
【図６】


20
30
21
31
UI読取手段
50
UI保持手段
23
24
32
33
鍵暗号化手段
鍵記録手段
ネットワーク
鍵読取手段
鍵復号化手段
22
D
34
鍵保持手段
鍵保持手段
10
25
26
35
36
40
入力手段
コンテンツ暗号化手段
コンテンツ記録手段
コンテンツ読取手段
コンテンツ復号化手段
出力手段

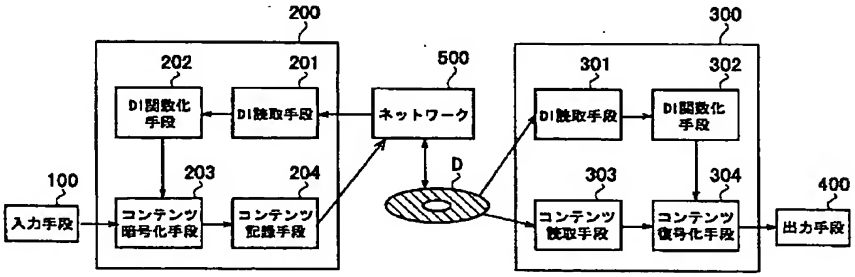
【図７】



【手続補正書】
【提出日】平成１１年７月２７日（１９９９．７．２７）
【手続補正１】
【補正対象書類名】図面
【補正対象項目名】図１
【補正方法】変更
【補正内容】
【図１】



【手続補正２】
【補正対象書類名】図面
【補正対象項目名】図４
【補正方法】変更
【補正内容】
【図４】



19　　20

フロントページの続き

(72)発明者　鈴木　英男
神奈川県横浜市神奈川区守屋町３丁目12番
地　日本ビクター株式会社内

Ｆターム(参考)　5D044 BC06 CC04 DE49 DE50 EF05
FG18 GK11 GK17 HL08